From New Scientist magazine
Saturday, May 15, 2004
USED WITH PERMISSION

They could turn out your lights, cut off your water and leave your phone line dead. Why are vital networks such as power grids and water supplies so vulnerable to hackers, and can one of the world's largest experiments prevent total meltdown? Duncan Graham-Rowe investigates.

Power play

By Duncan Graham-Rowe

In March 2001 Vitek Boden parked his car near a water treatment works at Pacific Paradise in Queensland, Australia. He switched on his laptop, typed a few commands and watched as 4.5 million liters of raw sewage spilt out into the waterways beside a nearby holiday resort. It turned the water black, poisoned marine life and created an overpowering stench.

Boden was an engineer formerly employed by the company that installed the computer system that controlled the water works. Bitter at missing out on a job at the local council, he exacted his revenge on the community by exploiting his knowledge of the works' control systems – with a little help from his wireless laptop connection. The police soon caught up with him and in October the same year he began a two-year stretch in jail.

Even though no lives were lost, it is the kind of incident that terrifies organizations such as the U.S. Department of Homeland Security. They don't see it simply as a sewage spill -- they see critical infrastructure under threat. If water treatment works are vulnerable to this kind of attack, then what about air transport or train networks, telephone systems, electricity grids and even, dare it be said, nuclear power plants?

The problem is that the control systems behind many public utilities are coordinated by outdated software with little or no protective firewall. Worse, these systems were designed to be accessed remotely. Experts are now extremely concerned that hackers, viruses or terrorists could easily gain access and disable critical services. The result could be chaos – or even massive loss of life.

To tackle the problem, the U.S. Department of Energy (DOE) is conducting what is probably the largest experiment in the world. Spanning 2300 square kilometers of desert near Idaho Falls, south of Yellowstone National Park, the Idaho National Engineering and Environmental Laboratory (INEEL) is equipped with a 50-megawatt power grid, hundreds of kilometers of high-voltage pylon, substations, chemical processing plants and even nuclear reactors. The plan is to use the site to test the control software that keeps the U.S., and much of the rest of the world, ticking over, in an urgent attempt to find and plug the gaps in the defenses before it is too late. The danger first came to light in 1997, during a cyber-war game organized by the Pentagon. Programmers and security experts realized that enemies, terrorists, or anyone with a grudge did not need to target military installations to cause chaos: they discovered that the civilian infrastructure that kept water and power flowing, for example, was far more vulnerable to cyber attack.

The result was Presidential Directive 63: Protecting America's Critical Infrastructures, issued by President Bill Clinton in May 1998. It called for the establishment of national centers that could warn of, and respond to, computer attacks, and also recommended a thorough search for any weaknesses in the software that controls the U.S. infrastructure. However, a combination of privatization and a continued lack of investment meant that by 2000, these vulnerabilities had still not been traced. The following year a task force of scientists and engineers was created to assess the full extent of the problem.

The challenge was huge. Computer simulations are useful, but without rehearsing attacks on a live system, no one could be sure how a network would respond. And of course, you can't play with parts of the real water supply or power grid without running the risk of genuine disruption. It is not even practical to isolate parts of a system to carry out limited tests, since this would put a huge strain on the rest of the network.

What was needed was a safe way of testing a variety of different hacking and virus attacks on a live control system. Such a system would need all the components of the genuine thing but without any of the associated perils if things went wrong. Building one network from scratch would cost a small fortune, but fortunately this proved unnecessary. The task force discovered that the DOE already had one in the form of INEEL.

Dotted across the vast site are labs, workshops and offices, as well as the high-voltage grid, waste management sites, nuclear reactors and a variety of wireless and fixed-line communication systems. INEEL even has its own fire, medical and meteorological services -- pretty much an entire nation in miniature, which is just what the task force needed. "They told us we don't even know what we have here," says Wayne Austad, a software engineer at INEEL.

The site grew up in the 1950s to serve the U.S.'s fledgling nuclear energy program. But over the years the power lines were co-opted to serve the 500-odd offices and buildings that sprang up alongside. By the late 1990s, it had become a fully functional grid serving a self-contained community of thousands of personnel. If the rest of the U.S. ground to a halt, this community would barely even notice. And more importantly for the task force, if the grid at INEEL went down, no one outside the site would suffer. "It's the only place in the world I know where you can do real testing of a grid," says Denise Swink, former acting director of the DOE's Office of Energy Assurance.

Engineers finally set to work on the tests last year, fitting INEEL's grid with dozens of sensors and "insertion points" – connections that allow them to monitor various parameters such as current and voltage, and to install software and run experiments on the grid's control systems.

The insertion points also ensure that the engineers can get accurate power readings at different points on the grid, to check whether the control software is actually doing what it says it is doing. The main object of their scrutiny is something experts agree is the most vulnerable part of almost every public utility network: a type of software program called a supervisory control and data acquisition system. SCADA gather and present data in real time, allowing operators to directly adjust a network or industrial production process on the fly, either from a control room or out in the field. For example, a SCADA can show staff the state of a pump or valve, the voltage on a capacitor or the fluid level in a tank, and the operator can make adjustments with just a few keystrokes.

For decades SCADA have controlled everything from floodgates to refineries, and gas pipes to driverless monorails or trains. The trouble is that they are not very well protected. "SCADA systems historically have no security in them," says Laurin Dodd, INEEL's head of security. This isn't simply an oversight. When SCADA appeared in the 1960s, the control networks on which they operated had no links to the outside world. What's more, SCADA were

designed to be as accessible as possible within these networks, so that engineers could tap in wherever they wanted.

Unfortunately communications technology and the networks on which SCADA operate have changed. In today's highly competitive markets, most water, power and transport networks are controlled in the cheapest way possible: via publicly available infrastructure such as telephone connections, the Internet and wireless links.

This might be good for profits, but from a security point of view it is a disaster. Most of the basic software components of SCADA remain unchanged, and have few security features such as firewalls to keep intruders out. And in most cases, you can't simply add protection to SCADA, as this could affect the way they work – an unacceptable risk when critical services are at stake. The problem is that utilities such as the electricity grid simply weren't designed to be this exposed. In fact the U.S. grid system was not really designed at all, says Dodd: it evolved out of several smaller, separate systems with very little consideration for security. "All they have in common is they are 110 volts," he says.

So how serious might the consequences of an attack be? Until the results of the tests come in, this is difficult to answer, but there is little doubt that many of the problems that affect the Internet could affect SCADA-based control networks. It's not just maverick hackers like Boden that pose a threat. There is the risk that computer viruses could disrupt operations too. For example, last June the North American Electric Reliability Council revealed that a computer worm had shut down a SCADA on the public electricity grid. And last year a safety system at the Davis-Besse nuclear power plant near Cleveland in Ohio was disabled by the Slammer worm.

Although the plant had no direct connection with external networks such as the Internet, it turned out that a contractor working on the system did. Fortunately the plant was offline at the time, but the incident served as a stark warning.

The security of nuclear reactors is certainly disturbing, but they wouldn’t necessarily be the first choice of someone searching for a vulnerable target, says Austad. A bigger concern is damage to a SCADA on the power grid, for example, which could unleash a cascade of failures. Since utilities are all interconnected, with power, telecommunications, business and finance depending upon each other, the result could be a nightmare costing billions to put right.

And it's not just a hypothetical scenario. On August 14, 2003, a power station at Eastlake by Lake Erie in Ohio suddenly went offline. The resulting domino rally of overloads ultimately left 50 million Americans and Canadians without power. Estimates suggest the blackout cost the U.S. and Canadian economies more than $10 billion.

Working with counterparts from Sandia National Laboratories in New Mexico, engineers at INEEL have already started to analyze their SCADA systems. They are initially testing a computer simulation of the power networks and their control systems using a host of specially developed hacking tools and viruses to see how the SCADA respond. Any chinks will then be investigated on isolated parts of the real INEEL grid. And if something causes significant disruption to the power supply, the engineers may expand the study to the entire grid.

Tests will include everything from releasing viruses to driving out into the desert and hacking into substations using a laptop with a wireless link. Even if a substation's SCADA system is password-protected or its wireless communication system uses powerful encryption software, the engineers need to be sure that something as simple as repeated attempts to connect – as might occur in a "denial of service" attack – won't make the control system play up or crash. And since the INEEL grid is bristling with sensors, the engineers can monitor the full effect of an attack and pick up any subtle knock-on effects.

This is complicated by the fact that there are many different types of SCADA out there, so the aim is to test the main products one by one, and advise manufacturers on how to create software or hardware patches for any weaknesses. It is a time-consuming process: to test and replace a single SCADA can take months. The process is expected to take eight years to complete, at a cost of $114 million.

Even so, Bill Flynt, former director of the U.S. Army's Homeland Security Threats Office, argues that this is not enough. It's not that vulnerable SCADA should not be patched, he says. In fact he agrees this is essential. But he says this is ultimately only a short-term solution: by merely patching SCADA you enter a kind of arms race. Attackers respond to countermeasures with new forms of attack, which then demand new fixes. The only way to make the power supply system truly secure, he argues, is to rebuild it from scratch. "This is a national security issue," Flynt says.

What is needed, he believes, is to make the network more resilient by using distributed architecture – something not unlike the self-healing structure of the internet which relies on a decentralized system of software and data stored on a huge number of machines round the globe.

At the moment, electricity in the U.S. is generated by relatively few large companies, whereas a distributed system would rely on huge numbers of small generators providing electricity for local communities, and feeding any excess power into the grid. It's not that this makes the whole thing more secure, but rather that it makes it more resilient. "The problems will be smaller and so more easily absorbed," Flynt says.

But Swink insists that rebuilding the grid in this way is just not economically feasible at present. Even if the requisite hundreds of billions of dollars were available, the transformation would take decades to complete. She argues that the tests at INEEL will allow companies to plug the holes in a reasonable time, without disrupting services.

The resulting system will be a little better at resisting cyber attacks by disgruntled employees with insider knowledge such as Boden. Whether it can keep out a determined terrorist armed with a laptop and wireless link remains to be seen.

Your country needs you

Rather than rebuilding vulnerable electricity grids, Robert Pratt at the Pacific Northwest National Laboratories (PNNL) at North Richland in Washington State reckons he has a better way to keep the current flowing. But if his plan is to succeed, we will all need to do our bit.

Pratt wants to install a special processor chip in every domestic appliance – washing machines, tumble dryers and so on. Developed at PNNL, the chip monitors the mains supply and if it detects that the grid is becoming overloaded, it reduces the energy load sucked up by the appliance. This small measure could go a long way, he says. In the U.S., appliances like fridges and dishwashers account for about 20 per cent of the grid's electrical load.

The chip works by sensing fluctuations in the frequency of mains electricity. In the U.S., this is usually maintained at 60 hertz, plus or minus 0.03 hertz. But if there is a sudden increase in demand for power, or a generator fails or there is a major distribution problem, the frequency can drop below 59.97 hertz. It may only take a few seconds for the electricity generators to correct this, but that can be enough to shut down whole sections of the grid.

However, when Pratt's chip senses a drop in mains frequency, it switches off the appliance. The chip can respond in less than half a second, much faster than generators can react. Put a chip in every fridge and dishwasher, and the nation could help keep the grid stable.

Initially the chip will be fitted in plugs so it would only be able to switch an appliance on or off. But Pratt hopes they will eventually be integrated into appliances to also adjust power consumption less crudely – keeping a washing machine's drum tumbling, for example, but turning off the heating element. He is currently conducting trials to show manufacturers that the chip won't damage their machines.

The chip could even be used to take the strain when supply outstrips demand – when loads are suddenly removed, for example. In theory, the PNNL chip could prevent this by switching on dishwashers and washing machines across the nation to soak up the excess power until the grid recovers. Who would pay the electricity bill, however, is another matter.

END OF ARTICLE

Duncan Graham-Rowe is a freelance journalist.